AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Ryan S. Burke, depose and state as follows:

AGENT BACKGROUND

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have been so employed since October 2012. I am currently assigned to the FBI's New Hampshire Resident Agency where I am tasked with investigating violent criminals and major offenders throughout the state. I primarily work alongside the Manchester Police Department ("MPD") as part of an initiative focused on reducing gun violence and other crime in the city of Manchester.

2. Throughout my career, I have led and/or been involved with investigations of robberies, kidnappings, murders, fugitives, extortions, threats, drug distribution, illegal possession of firearms, and other crimes. My investigations have included the use of the following investigative techniques: physical surveillance; handling of cooperating sources and witnesses; exploitation of cellular, social media, and Internet Protocol ("IP") based communications data; execution of search and seizure warrants; wire, electronic, and oral wiretaps; and the execution of arrest warrants.

3. Based on my training, experience, and information provided to me by other law enforcement officers, I am familiar with the modus operandi used by individuals engaged in the violation of various criminal offenses, such as those related to acts of violence, firearms, and controlled substances. For example, I have handled many cooperating sources and witnesses who have provided information to me specifically related to shootings, the distribution of controlled substances, and various firearms offenses. I have also reviewed thousands of court-authorized wiretap intercepts between drug traffickers, violators of firearm offenses, individuals conspiring to commit armed robberies, and individuals engaged in the violation of other offenses. Many of

these investigations have resulted in the execution of search warrants, arrest warrants, and eventual convictions.

PURPOSE OF AFFIDAVIT

4. I submit this affidavit in support of an application for a warrant to search the following premises (hereafter, the "**Target Premises**"):

a. Unit 2 of the multi-unit, three-story, yellow building located at 141 Orange Street in Manchester, New Hampshire.

5. Based on the information contained herein, there is probable cause to believe that the **Target Premises** contains evidence, fruits, and instrumentalities of the crime of 18 U.S.C. § 922(g)(1) [Felon in Possession of Ammunition & Firearm].

6. The information set forth in this affidavit is based on my personal participation in this investigation, as well as my training and experience, and information received from other law enforcement officers. I have not set forth every detail I or other law enforcement officers know about this investigation but have set forth facts that I believe are sufficient to evaluate probable cause as it relates to the issuance of the requested warrant.

PROBABLE CAUSE

7. On August 19, 2021, Ethan Lea (YOB: 1990) was arrested in Loudon NH pursuant to an active state warrant for Controlled Drug Violations. He was subsequently transported to MPD for processing and to be interviewed. Prior to the interview, Lea was informed of his Miranda rights, acknowledged his understanding of those rights, and signed a form to memorialize his willingness to answer questions without an attorney present. In the audio-video recorded interview that followed, Lea provided, amongst other things, information related to a firearms transaction that took place at the **Target Premises**.

8. Between sometime in April 2021 when Lea was released from prison and approximately July 2021, Lea was present at the **Target Premises** for a meeting with Ryan Call (YOB: 1986), Gina Cecere (YOB: 1997), and Sean Dauria (YOB: 1983). Based on a review of the criminal histories for Lea, Call, Cecere, and Dauria, I know they have each been convicted of one crime or more punishable by imprisonment for a term exceeding one year. Therefore, each individual is federally prohibited from possessing firearms.

9. According to Lea, during the meeting, Call instructed Dauria to retrieve two assault rifles and a shotgun from an unknown location in New Hampshire and bring them to the **Target Premises**, which he did. When Dauria arrived at the **Target Premises**, Lea observed the three firearms and handled at least one of them. Lea also observed Call pay an unknown amount of money to Dauria for retrieving the firearms.

10. During approximately the second week of August 2021, Lea contacted Cecere and asked her if she still had any of the firearms. Lea's inquiry was based on his knowledge that Call had been arrested in early July 2021 and remained in custody. Cecere informed Lea at that time that she was still in possession of at least one rifle.

11. MPD in-house records for individuals associated with the **Target Premises** confirmed Cecere was the primary occupant, as described by Lea. In fact, on May 24, 2021, Cecere was arrested inside the **Target Premises,** which she described as her home. Furthermore, on August 24, 2021, law enforcement observed Cecere exit 141 Orange Street, which further substantiated her continued occupancy of the **Target Premises**. Cecere had previously been convicted of a felony Controlled Drug Violation [RSA 318-B:2] in Hillsborough County (NH) Superior Court – North, and is therefore prohibited from possessing firearms.

12. Based on the foregoing, I believe the **Target Premises** will contain one or more firearms and ammunition evidencing violations of 18 U.S.C. § 922(g)(1) [Felon in Possession of Ammunition & Firearm], and/or electronic devices containing content and communications evidencing such violations.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

13. As described in Attachment B, this application seeks permission to search for records that might be found on the **Target Premises**, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the

Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

15. *Probable cause.* I submit that if a computer or storage medium is found on the **Target Premises**, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the **Target Premises** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the

storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that

log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

17. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or

imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

19. Because it is likely that several people share the **Target Premises** as a residence, it is possible that the **Target Premises** will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

AUTHORIZATION TO USE BIOMETRIC FEATURES TO UNLOCK DEVICES

20. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant.

21. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device

through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

22. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

23. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

24. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

25. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

26. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time.

27. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours and the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

28. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose physical characteristics are among those that will unlock the device via biometric features, and it

is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any individual, who is found at the subject Target Premises and reasonably believed by law enforcement to be a user of the device, to unlock the device using biometric features in the same manner as discussed above.

29. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject Target Premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.

AUTHORIZATION TO COLLECT DNA SAMPLES

30. Because the **Target Premises** may be occupied by numerous individuals, I respectfully request authorization to obtain DNA (Deoxyribonucleic acid) samples from Cecere and other permanent residents. The DNA samples would be used for comparative analyses of any firearms, ammunition, or other items seized from the **Target Premises**, and any other relevant items collected during the course of this investigation. The request to collect DNA samples from

Cecere is subject to her presence at the **Target Premises** during the execution of the requested warrant.

CONCLUSION

31. I submit that this affidavit supports probable cause for a warrant to search the **Target Premises** described in Attachment A and seize the items described in Attachment B. The seizure of these items will aid law enforcement in their investigation of various violations of 18 U.S.C. § 922(g)(1) [Felon in Possession of Firearm/Ammunition].

REQUEST FOR SEALING

32. I request that the Court order that all papers in support of these applications, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public and/or known to all parties relevant to the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

/s/ Ryan S. Burke
Ryan S. Burke, Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: 8/25/21
Time: 11:28 am

HONORABLE DANIEL J. LYNCH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

Unit 2 of the multi-unit, three-story, yellow building located at 141 Orange Street in Manchester, New Hampshire.

The premises to be searched includes the main residence and all attached and unattached rooms, attics, basements, garages and storage areas, floor, wall and combination safes, lockers, briefcases, containers, trash areas, and outbuildings assigned to or part of the particular apartment; surrounding grounds and common areas/staircases; as well as the persons of adults located at the premises at the time of the execution of this search warrant.

ATTACHMENT B

Description of Information or Items to Be Seized

I. All records, in whatever form, and tangible objects that constitute evidence, fruits, or instrumentalities of 18 U.S.C. § 922(g)(1) [Felon in Possession of Ammunition & Firearm], including information and items related to:

a. Firearms, weapons, ammunition, and firearms-related accessories;

b. DNA sample(s) from occupants of Unit 2 of 141 Orange Street, Manchester NH;

c. United States currency, foreign currencies, and other forms of currency acquired or used during transactions involving contraband;

d. Places and locations where evidence of the above-referenced criminal offenses was obtained or discarded, or is currently stored;

e. The identities of any co-conspirators, as well as any co-conspirators' acts taken in furtherance of the offenses enumerated in this application;

f. Electronic devices, including mobile electronic equipment, serial numbers or any electronic identifiers that serve to identify the equipment, and the information stored electronically on the devices, specifically:

i. telephone logs, contact lists, other records reflecting names, aliases, addresses, telephone numbers, and other contact or identification data;

ii. the actual and attempted possession, purchase, receipt, sale, pawn, trade, transfer, transportation, shipment, or other disposition of firearms and ammunition, including buyer lists, seller lists, notes, pay-owe sheets, records of sales, logs, receipts, and communications;

iii. messages and other communications related to firearms violations;

iv. photographs, images, and depictions of or related to firearms violations and currency;

v. who used, owned or controlled the equipment;

vi. when the equipment was used;

vii. the travel and whereabouts of the user of the equipment;

viii. the attachment of other hardware or storage media;

ix. the use of counter-forensic programs and associated data that are designed

to eliminate data;

x. passwords, encryption keys, and other access devices that may be necessary to use the equipment;

xi. accounts associated with software services or services providing Internet access or remote storage of either data or storage media; and

xii. serial numbers and any electronic identifiers that serve to identify the equipment.

II. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. Items described in Paragraph I (a) through (f);

b. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

f. evidence indicating the computer user's state of mind as it relates to the crimes under investigation;

g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

i. evidence of the times the COMPUTER was used;

j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

l. records of or information about Internet Protocol addresses used by the COMPUTER;

m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

n. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" (or "COMPUTER") includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

During the execution of the search of the property described in Attachment A, law enforcement officers are authorized to press or swipe the fingers (including thumbs) of any individual, who is found at the subject Target Premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; and/or (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search its contents as authorized by this warrant.